REMARKS

In the Claims

Claims 1-13 were rejected under 35 USC § 103 based on various cited references, including U.S. Patent No. 5,757,912 to Blow ("Blow") and U.S. Patent Application Publication No. 2003/0112970 to Mitra ("Mitra").

Claims 6 and 9-13 have been canceled so that claims 1-5 and 7, 8 are now pending in the application.

Claim amendments

Claims 1, 5, 7 and 8 have been amended.

In response to Examiner's comment #6 on page 3 of the Office Action, independent claims 1, 5 and 8 have been amended to expressly claim that the invention is directed to establishing an ***initial quantum key***.

Claims 1, 5 and 8 have also been amended to indicate that ***the QKD stations initially have no shared quantum key***.

Independent claims 1 and 5 have also been amended to also include all of the steps used to establish the initial quantum key rather than just the steps used to form "encrypted qubits."

Similarly, claim 8 has been amended to add first and second operably coupled controllers at Alice and Bob respectively, "wherein the first and second controllers are configured to run QKD procedures to establish an initial quantum key from the first key bits and the recovered second key bits."

Thus, all of the independent claims include all of the steps used to form an initial quantum key, along with the limitations that the QKD stations initially have no shared quantum key and that the result is an initial quantum key.

Applicants incorporate by reference herein the arguments made in the previous office action, and offer the following clarifying comments with respect to the presently pending claims.

Claims 1

Independent claim 1 was rejected under 35 USC § 103 based on Blow in view of Mitra.

Applicants maintains that Mitra is unmistakably concerned with ***encrypting existing keys to form new keys***, and so does not disclose any of the claim limitations of Applicants' claim 1 as presently amended, which directed to forming ***an initial quantum key*** based on transmitting encoded weak light pulses between first and second QKD stations that initially do not share a quantum key.

Mitra in combination with Blow is ***inoperable*** with respect to carrying out Applicants' claimed invention because Mitra assumes that a key is already shared between Alice and Bob before it performs the encryption step to form the "double encrypted key" (see Mitra, Paragraph [0013]). One skilled in the art would clearly understand Mitra describes "post-processing" step on keys that are already shared, much in the manner of performing key sifting, error correction and privacy amplification on an initial quantum key to form a more refined, secure key. Such steps, however, have no utility in and are entirely inapplicable to forming an ***initial quantum key between QKD stations that initially do not share a quantum key***.

The Summary of the Invention section of Mitra (paragraphs [0011]-[0016]) describes the general approach of how Alice and Bob go about encrypting the existing keys, which are made of "key bits." Applicants hasten to note here that the term "key bits" as used by the Applicants is ***different*** than in Mitra. In Applicants' invention, the term "key bits" refers to randomly generated bits used to randomly encode the weak light pulse ultimately used to establish the initial quantum key. In Mitra, a "key bit" is a bit that makes up an existing key.

It is readily apparent from Mitra paragraphs [0011]-[0016] that the encrypting method of Mitra could not possibly be applied to Applicants' claim 1. In Mitra, ***Alice and Bob must already have a shared key K(2n),*** and the method of Mitra requires the use of this shared key to form sub-keys, which are then used to encrypt a secret message. In Applicants' claimed invention, Alice and Bob go about forming an initial quantum key without the benefit of having a shared quantum key. Once the initial

quantum key is formed, the methods of Mitra could perhaps be used to further process the quantum key, but ***there is simply no hope of ever getting the invention of Mitra to be operable in forming the initial quantum key because by definition Mitra needs the initial quantum key to operate***.

Applicants respectfully submit that amended claim 1 clarifies the distinguishing features discussed above and render claim 1 (and thus claims 2-4 depending therefrom) patentable over the cited prior art.

Claim 5

Claim 5 is rejected for essentially the same reasons as claims 1, and further in view of the article "Applied Cryptography" by Schneier ("Schneier").

Applicants submit that claim 5 as amended is patentable over the cited prior art for essentially the same reasons as set forth above in connection with claim 1. Claim 7 depending therefrom is therefore also patentable over the cited prior art.

Claim 8

Claim 8 is rejected under 35 USC §103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend ("Townsend") in view of U.S. Patent Application Publication No. 2006/0120529 to Gisen et al. ("Gisen"), and further in view of Schneier and Mitra.

Applicants submit that
claim 8 as amended is patentable over the cited prior art for essentially the same reasons as set forth above in connection with claim 1.

CONCLUSION

Claims 1-5, 7 and 8 are now pending in the Application. Applicants respectfully submit that the presently pending claims are patentable over the cited art in view of the amendments to these claims and the reasons set forth above. Applicants' therefor respectfully submit that claims 1-5, 7 and 8 as presently presented are in condition for allowance and earnestly request a Notice of Allowance be issued in due course.

The Examiner is encouraged to contact the undersigned Attorney at 941-378-2744 to discuss any questions that may arise in connection with this Amendment.

Respectfully Submitted,

By: _____ Date: July 28, 2009

Joseph E. Gortych

Reg. No. 41,791

Customer No. **53590**

Opticus IP Law PLLC
7791 Alister Mackenzie Dr
Sarasota, FL 34240 USA

Phone: 941-378-2744
Fax: 321-256-5100
E-mail: jg@opticus-ip.com